IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. DOMINIQUE ALEXANDER PIATTI, an individual; DOTFREE GROUP S.R.O., a Czech limited liability company, and ANDREY N. SABELNIKOV, an individual, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS Defendants.	Civil Action No: 1:11cv1017 (JCC/IDD)

FIRST AMENDED COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against Defendant ANDREY N. SABELNIKOV ("Defendant"), controlling the "Kelihos" botnet using twenty-one (21) Internet domain names set forth at Appendix A to this Complaint including, in particular, the 3,723 "cz.cc" Internet sub-domains identified at Appendix B to this Complaint (collectively the "Harmful Botnet Domains") as follows:[1]

NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) CAN-SPAM Act, 15 U.S.C. § 7704; (3) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (4) False Designation of Origin under The Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under The Lanham Act, 15 U.S.C. § 1125(c); (6) Common Law Trespass to Chattels; (7) Unjust Enrichment; and (8) Conversion. Microsoft seeks injunctive and other equitable relief and damages against Defendant as the operator of a controlled network of

[1] The first two named Defendants in the caption, Dominique Alexander Piatti and DotFree Group S.R.O. were previously dismissed from this action.

computers, known as the "Kelihos" botnet, by means of the Harmful Botnet Domains that have and continue to cause irreparable injury to Microsoft, its customers, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. Defendant Andrey N. Sabelnikov is an individual residing in St. Petersburg, Russian Federation. Defendant currently works on a freelance basis for a software development and consulting firm. Prior to his current employment, Defendant worked as a software engineer and project manager at a company that provided firewall, antivirus and security software. Defendant has a degree from the Department of Computer Systems and Programming, St. Petersburg State University of Aerospace Instrument Engineering.

4. Microsoft is informed and believes and thereupon alleges that Defendant wrote and/or participated in creating the harmful computer software that constitutes the Kelihos botnet and that Defendant has used the software to control, operate, maintain and grow the Kelihos botnet, by among other things, infecting innocent users' computers. The harmful computer software used to control the Kelihos botnet contains information that identifies Defendant and demonstrates that Defendant created, operated and controlled the Kelihos botnet.

5. Microsoft is informed and believes and thereupon alleges that Defendant owns, operates, controls and maintains the Kelihos Botnet and does business under the names of the Harmful Botnet Domains. Microsoft is informed and believes and thereupon alleges that Defendant is responsible for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by Defendant.

6. Third parties Dominique Alexander Piatti ("Mr. Piatti"), an individual, and dotFree Group s.r.o. ("dotFree Group"), a Czech limited liability company, are identified as the registrants of the top-level Internet domain "cz.cc." Mr. Piatti and dotFree Group s.r.o. use the "cz.cc." domain to register other Internet domains (known as "sub-domains"), such as

"cyvgtbxa.cz.cc." Microsoft is informed and believes and thereupon alleges that Defendant purchased at least 3,723 "cz.cc" based sub-domains from Mr. Piatti and dotFree Group, set forth at Appendix B to this Complaint, and misused said sub-domains to operate and control the Kelihos Botnet and to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that Mr. Piatti and dotFree Group are located at Prazska 636, Dolni Brezany, Praha-Zapad 25241, Czech Republic.

7. Third party Internet.bs Corp. is a domain name registrar through which some of the Harmful Botnet Domains are registered. Microsoft is informed and believes and thereupon alleges that Defendant purchased ".com" domains through Internet.bs Corp., set forth at Appendix A to this Complaint, and misused said domains to operate and control the Kelihos Botnet and to cause harm to Microsoft, its customers, and the public. Internet.bs is located at 98 Hampshire Street, N-4892 Nassau, The Bahamas.

8. Third party Verisign, Inc. is the domain name registry that oversees the registration of all domain names ending in ".cc" and ".com," including all of the Harmful Botnet Domains, and is located at 21345 Ridgetop Circle, Dulles, Virginia, 20166, in the Eastern District of Virginia.

9. The actions and omissions alleged herein to have been undertaken by the Defendant were undertaken Defendant individually, were actions and omissions that Defendant authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions that Defendant assisted, participated in, or otherwise encouraged, and are actions for which Defendant is liable. Defendant aided and abetted the actions of others, alleged herein, had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part.

JURISDICTION AND VENUE

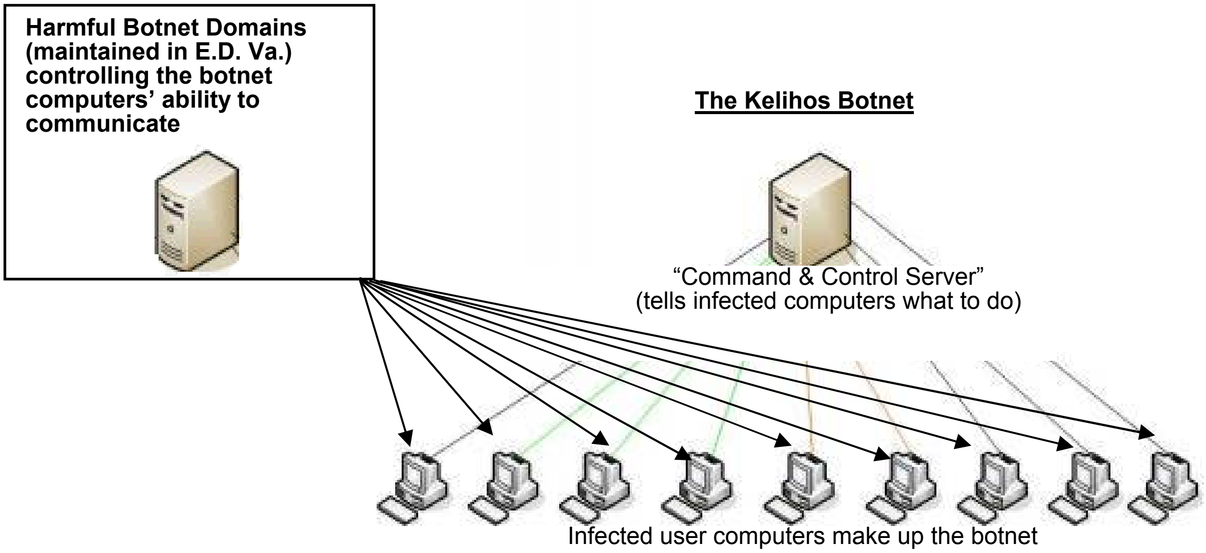
10. This action arises out of Defendant's violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701) and the Lanham Act (15 U.S.C. § 1125).

Therefore, the Court has subject matter jurisdiction of this action based on 28 U.S.C. § 1331. This is also an action for trespass to chattels, unjust enrichment and conversion. Accordingly, this Court has subject matter jurisdiction under 28 U.S.C. § 1367.

11. Upon information and belief, Defendant created the harmful malware that constitutes the Kelihos botnet; has maintained computers and Internet websites; has engaged in other conduct availing himself of the privilege of conducting business in Virginia; has directed acts complained of herein toward Virginia; and has utilized instrumentalities located in Virginia to carry out the acts complained of herein.

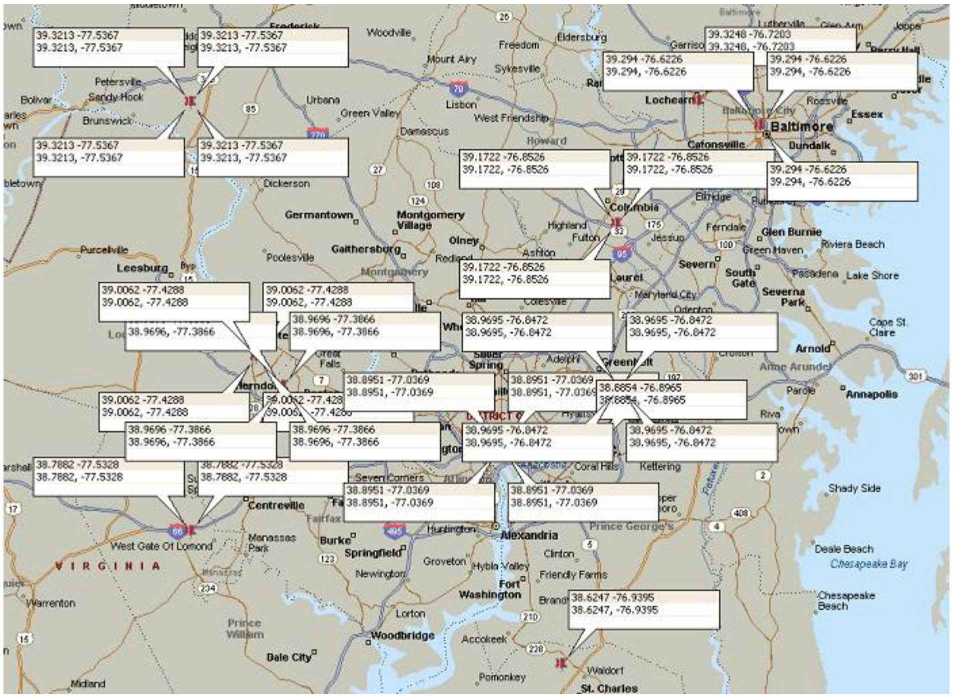
12. Defendant has used or maintained twenty-one (21) ".com" Internet domains and at least 3,723 sub-domains under the "cz.cc" Internet domain, collectively referred to herein as the Harmful Botnet Domains, specifically registered through Verisign in Virginia. Defendant harms Microsoft, its customers, and the public through the Harmful Botnet Domains. Defendant uses the Harmful Botnet Domains to control the communications of a network of compromised user computers, called a "botnet," which Defendant owns, operates, and maintains to cause harm to Microsoft, its customers, and the public.

13. The following represents the relationship of the Harmful Botnet Domains registered through facilities in the Eastern District of Virginia to the "botnet."


Harmful Botnet Domains (maintained in E.D. Va.) controlling the botnet computers' ability to communicate
The Kelihos Botnet
"Command & Control Server" (tells infected computers what to do)
Infected user computers make up the botnet

14. Defendant has also directed actions at Virginia, including specifically the Eastern

District of Virginia, by directing malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia, infecting those user computers with the malicious code and thereby making the user computers part of the "botnet," which is used to injure Microsoft, its customers and the public. The following depicts the geographical location of user computers in Virginia at which Defendant is known to have directed malicious code, causing those computers to become infected and part of the botnet:



15. Defendant has undertaken the foregoing acts with knowledge that such acts would cause harm through the ".com" and "cz.cc" domains and sub-domains located in Virginia and through user computers located in Virginia, thereby injuring Microsoft, its customers, and others both in Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendant.

16. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Microsoft's claims, together with a substantial part of the property that is the subject of Microsoft's claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(b) because a domain name is deemed to have its situs in the judicial district in which the domain name

registry that registered or assigned the domain name is located. Verisign is the domain name registry for the Harmful Botnet Domains and is located in this district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because the Defendant is subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

Microsoft's Software, Services And Reputation

17. Microsoft® is a provider of the Windows® operating system and the Hotmail®, Windows Live® and MSN® e-mail and messaging services and a variety of other software and services. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Microsoft®, Windows®, Hotmail®, Windows Live® and MSN® marks.

Computer "Botnets"

18. In general, a "botnet" is a collection of individual computers, each running software that allows communication among those computers and allows centralized or decentralized communication with other computers providing control instructions. The individual computers in a botnet often belong to individual users who have unknowingly downloaded or been infected by the software (known as malicious software or malware) that makes the computer part of the botnet. For example, an end-user's computer may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment or downloads malicious software. In each such instance, software code is downloaded or executed on the user's computer, causing that computer to become part of the botnet, capable of sending and receiving communications, code and

instructions to or from other botnet computers.

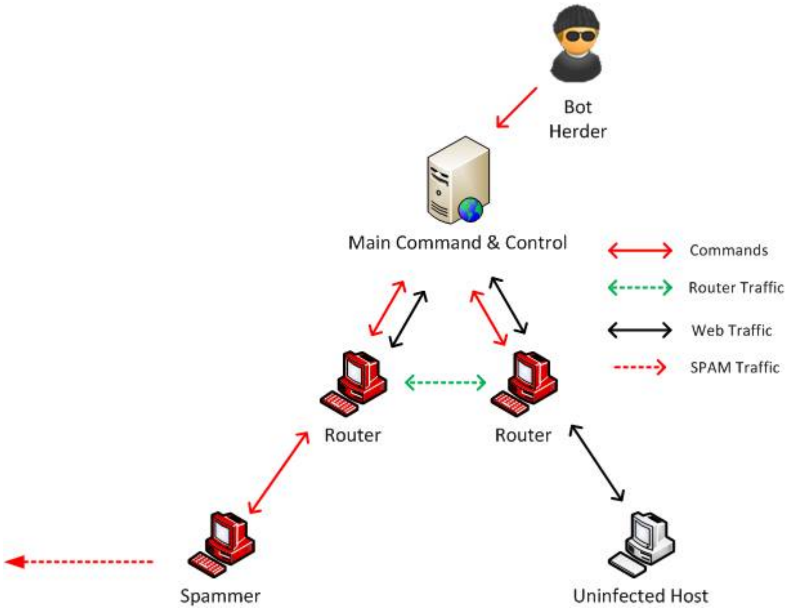
19. Some botnet computers are wholly within the control of the botnet creator. These may have specialized functions, such as sending control instructions. These may be referred to as "command and control" computers.

20. Botnets are often created and controlled by sophisticated organizations and are used to carry out misconduct that harms others' rights. For example, a computer in a botnet may be used to anonymously send unsolicited, bulk email without the knowledge or consent of the individual user who owns the compromised computer. Similarly, a botnet computer may be used to deliver further malicious software that infects other computers, making them part of the botnet as well. A botnet computer may also be used to carry out fraud, computer intrusions or other misconduct. A botnet computer may also be used simply to "proxy" or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications.

The "Kelihos" Botnet: Overall Architecture

21. Microsoft brings this action to stop Defendant from harming Microsoft and its customers through the malicious use of the Harmful Botnet Domains which are central to a botnet known as the "Kelihos" botnet. A high-level depiction of the relationship between the Harmful Domains and the Kelihos Botnet is set forth above.

22. The Kelihos Botnet has a multi-tiered architecture, represented as follows:



23. The lowest "Spammer Node" tier in this architecture is made up of infected user computers that have been determined to be behind firewalls or otherwise not directly accessible from the Internet. These infected user computers are essentially the workers of the botnet, perform the day-to-day illegal activity. Critically, the malicious software placed on these infected computers sends, without the user's knowledge or permission, unsolicited bulk email (often known as "spam"). This spam email may contain code that infects further computers adding them to the botnet or may serve other purposes, such as inviting users to enter financial or other valuable personal information. The botnet selects user computers behind firewalls to act as the "Spammer Nodes" because such computers are more difficult to monitor or to reach remotely to remediate the problem. The sending of spam email is a major component of the Kelihos Botnet's functionality.

24. The next highest tier in the architecture, the "Router Node" tier, is made up of infected computers that are directly accessible from the Internet. These computers may serve several different purposes, depending on the instructions sent by the botnet's command and control computers. First, they may act as proxies relaying communications among different botnet computers, both to distribute the processing burden and to obfuscate the true source of the communications. Second, these computers may act as HTTP, SOCKS 4 or SOCKS 5 servers capable of delivering commands and responses, when receiving requests from other botnet computers. These computers act as proxies for both infected computers already part of the botnet as well as uninfected computers that are following a URL received in a spam email message. Third, these computers may act as "DNS servers." In general, a DNS server is a computer that translates human readable hostnames or domain names (such as magdali.com) to their corresponding binary identifier, called an IP address (such as 46.37.195.161).

25. At the highest level, there are one or more command and control servers, referred to as the "Main Command & Control" servers. Upon information and belief, these servers are controlled directly by Defendant and not made up of infected computers. The Main Command & Control servers are responsible for coordinating the Kelihos Botnet on the whole and providing

the most fundamental definitions, commands and instructions that determine how infected computers will operate and how different botnet components will interact with each other.

26. Microsoft is informed and believes and thereupon alleges that Defendant wrote and/or participated in creating the code in each of foregoing tiers of the Kelihos Botnet.

The Kelihos Botnet: The Harmful Botnet Domains

27. The Kelihos Botnet uses a method called "fast flux" hosting, which is a technique used by botnets to hide the location of their constituent computers by constantly changing the addressing of the domain names that are associated with the command and control and infrastructure components that make up the botnet. The purpose and result of fast flux hosting is that discovery, observation and counter-measures are made more difficult because the addressing of the constituent compromised computers is constantly changing.

28. The Kelihos Botnet uses fast flux hosting technique to obfuscate the source, location, owner and other attributes of the computers providing command and control to the botnet. The fast flux infrastructure accomplishes this by regularly updating the root name servers for the various fast flux domains used by the Kelihos Botnet. As a result, the Defendant is able to continuously obscure the attributes of these Kelihos domains.

29. Each of the Harmful Botnet Domains set forth in Appendices A and B are one of the foregoing described fast flux Kelihos domains, representing a component in the command and control of the botnet. Upon information and belief, the purpose of each of the Harmful Botnet Domains set forth in Appendices A and B is to support and propagate the Kelihos Botnet and further its malicious activity.

30. The computers that are part of the Kelihos Botnet can send "node table updates" to other computers in the botnet. These node table updates contain lists of other known Router Nodes, to enable and support continued communication between all of these computers. The communication from the Spammer Node tier to the Router Node tier and communication between Router Nodes depends on the accuracy of the node tables stored at each computer and depends on the accuracy of node table updates. If a node table is empty or contains invalid

entries, a given botnet computer uses a specified IP address, which is hardcoded in the Kelihos botnet software residing on the infected computer, to query the botnet for an update to the node table. If for any reason, a Spammer Node or Router Node computer is unable to communicate with the IP addresses, the given botnet computer – as a failsafe – will use one of the Harmful Botnet Domains, which is also hardcoded in the Kelihos botnet software residing on the infected computer, to query the botnet for an update to the node table. Thus, the Harmful Botnet Domains continuously control the ability of the computers that make up the Kelihos Botnet to communicate with each other and to grow the botnet.

Injury Caused By The Kelihos Botnet To Microsoft And Its Customers

31. In addition to supporting Kelihos Botnet's infrastructure, as described above, the Harmful Botnet Domains may further be used in at least the following way. Links to those domains may be included in unsolicited, bulk email sent out by Spammer Node computers with the purpose of spreading the botnet. For example, the Spammer Node computers have been observed to send emails indicating to the victim recipients that a loved one has sent the victim an e-card. The emails point to one of the Harmful Botnet Domains, which represents a Router Node computer. When the victim opens the link sent to them, in order to retrieve the e-card, the victim is interacting directly with the Router Node computer, which may deliver malicious software that infects the victim's computer and makes it part of the Kelihos Botnet.

32. The malicious Kelihos Botnet software is clandestinely introduced onto users' computers, infecting those computers and making them part of the botnet. These acts constitute an unauthorized intrusion into the Microsoft Windows® operating system which Microsoft licenses to the end users. In particular, the Kelihos Botnet specifically targets the Windows® operating system. For example, the Kelihos Botnet writes particular entries to the registry of the Windows® operating system, without the consent of Microsoft or its customers, including commands that tell the computer which commands to execute, commands that facilitate communication between botnet computers, commands which harvest personal email addresses from the computer, commands that tell the computer how to receive instructions from Defendant

and data identifying the computer within the botnet. The spread of the Kelihos Botnet in this way is not related to any vulnerability in Microsoft's systems, but is instead achieved by misleading unwitting users into taking steps that result in the infection of their machines.

33. The Kelihos Botnet's intrusion into Microsoft's Windows® operating system is without the authority of Microsoft and exceeds any authority granted by Microsoft to any party, including the end-user and Defendant.

34. The Kelihos Botnet harms Microsoft's customers by misusing the Windows® operating system on those users' infected computers. The Kelihos Botnet causes harm to Microsoft's customers by, among other things, causing customers' computers to:

a. install and run software without the customers' knowledge or consent, including software to support the botnet infrastructure, software that causes the computer to act as an HTTP Proxy, an HTTP Server, a DNS Server, a SOCKS 4 Proxy, a SOCKS 5 Proxy, software that acts as an SMTP email engine, software enabling the computer to initiate a DDoS attack, and an HTTP P2P Engine;

b. have deteriorated performance due to the running of unauthorized software;

c. install and run software without the customers' knowledge and consent which collects personal information, including personal email address information of the customers and others;

d. send spam email to others, including users of Microsoft's Hotmail email account holders and users of Microsoft's Outlook email program;

e. transmit collected personal information, including personal email address information and other information, to the Kelihos Botnet Main Command & Control Server

35. The unauthorized access of and intrusion into Microsoft's Windows® operating system and Microsoft's customers' computers results in consumer confusion. Microsoft's customers have notified Microsoft of damage caused by the Kelihos Botnet and the Harmful Botnet Domains. Such customers have been confused and have been incorrectly led to believe

that Microsoft was the source of damage and therefore attributed their injury to Microsoft and its products and services. Thus, the Kelihos Botnet and the Harmful Botnet Domains have caused injury to Microsoft's brand, reputation and goodwill. This incorrect attribution of the effects of the Kelihos Botnet and the Harmful Botnet Domains to Microsoft causes harm to Microsoft's brand and tarnishes the reputation of Microsoft's name, products and services. Microsoft has had to expend substantial resources in an attempt to assist its customers and to correct the continuing misperception that Microsoft is the source of damage caused by the Kelihos Botnet and the Harmful Botnet Domains.

36. Upon information and belief, the Defendant who operates the Kelihos Botnet benefits from its operation and the activities described above by sending spam email, which generates advertising revenue, and by selling to others, for profit, the botnet's capability of sending unsolicited, bulk email and carrying out other activities on behalf of others.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

37. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 36 above.

38. Defendant: (a) knowingly and intentionally accessed Microsoft customers' protected computers and Microsoft's protected computers without authorization or in excess of any authorization and thereby obtained information from the protected computers in a transaction involving an interstate or foreign communication (18 U.S.C. § 1030(a)(2)(C)), (b) knowingly and with an intent to defraud accessed the protected computers without authorization or in excess of any authorization and obtained information from the computers, which Defendant used to further the fraud and obtain something of value (18 U.S.C. § 1030(a)(4)); (c) knowingly caused the transmission of a program, information, code and commands, and as a result of such conduct intentionally caused damage without authorization to the protected computers (18 U.S.C. § 1030(a)(5)(A)); and (d) intentionally accessed the protected computers without authorization, and as a result of such conduct caused damage and loss (18 U.S.C. § 1030(a)(5)(C)).

39. Defendant's conduct has caused a loss to Microsoft during a one-year period aggregating at least $5,000.

40. Microsoft has suffered damages resulting from Defendant's conduct.

41. Microsoft seeks compensatory and punitive damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

42. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

SECOND CLAIM FOR RELIEF

Violation of CAN-SPAM Act, 15 U.S.C. § 7704

43. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 36 above.

44. Microsoft is a provider of internet access service. Microsoft enables users to access content, including proprietary content, electronic mail, and other internet services.

45. Defendant initiated the transmission of unsolicited, bulk email, which are commercial electronic messages, by means of the Kelihos Botnet, through Microsoft customers' computers and through Microsoft's computers, which are used in interstate and foreign commerce and communication, to thousands or millions of computers, which are also used in interstate and foreign commerce and communication and are "protected computers" as defined by 18 U.S.C. § 1030(e)(2)(B).

46. By sending messages by means of the Kelihos Botnet, Defendant initiated the transmission of commercial electronic mail messages, to protected computers that contained materially false or misleading header information in violation of 15 U.S.C. § 7704(a)(1).

47. Defendant initiated the transmission of commercial electronic messages to protected computers with actual or fairly implied knowledge that the subject headings of the messages would likely materially mislead recipients regarding the contents or subject matter of the message in violation of 15 U.S.C. § 7704(a)(2).

48. Defendant transmitted to protected computers commercial email messages that did not contain a functioning return electronic mail address or other Internet-based mechanism that recipients could use to contact Defendant and indicate their desire to opt-out of future messages from Defendant, in violation of 15 U.S.C. § 7704(a)(3).

49. Defendant initiated the transmission to protected computers of commercial electronic messages that did not provide (a) clear and conspicuous identification that the message was an advertisement or solicitation; (b) clear and conspicuous notice of the right to decline to receive future message; or (c) a valid physical postal address of the sender, in violation of 15 U.S.C. § 7704(a)(5).

50. Defendant's unsolicited, bulk emails were sent as part of a systematic pattern and practice that did not conspicuously display a return electronic mail address by which the recipients could submit to the true sender a reply requesting that no further commercial emails be sent to the recipient.

51. As a direct result of Defendant's actions, Microsoft has suffered harm in an amount to be determined at trial.

52. Microsoft is entitled to the greater of actual damages or statutory damages in accordance with 15 U.S.C. § 7706(g)(1)(B).

53. On information and belief, Defendant's actions were willful and knowing, entitling Microsoft to aggravated damages in accordance with 15 U.S.C. § 7706(g)(3)(C).

54. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

THIRD CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

55. Microsoft realleges and incorporates by reference the allegations contained in paragraphs 1 through 36 above.

56. Microsoft's computers and servers and its licensed operating system are facilities

through which electronic communication service is provided to its users and customers.

57. Defendant knowingly and intentionally accessed Microsoft customers' computers and Microsoft's computers and servers without authorization or in excess of any authorization granted by Microsoft.

58. Through this unauthorized access, Defendant had access to, obtained, altered, and/or prevented Microsoft's users' and customers' legitimate, authorized access to wire electronic communications, including but not limited to emails while they were in electronic storage in the computers and servers of Microsoft and its customer and within Microsoft's licensed operating system.

59. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

FOURTH CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

60. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 36 above.

61. The marks "Microsoft," "Windows," "Windows Live," "MSN" and "Hotmail" ("Microsoft Marks") are distinctive marks that are associated with Microsoft and exclusively identify Microsoft's business, products, and services.

62. The Kelihos Botnet creates keys and writes entries to the Windows® registry. By creating keys and writing entries under a registry path that includes the Microsoft Marks, Defendant is likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the malicious software installed by the Kelihos Botnet, including through the Harmful Botnet Domains.

63. The Harmful Botnet domains include and use the Microsoft Marks, as subdomains or as content available through the domains. By including and using the Microsoft Marks as subdomains or as content available through the domains, Defendant is likely to cause

confusion, mistake, or deception as to the origin, sponsorship, or approval of the domains.

64. By using the Microsoft Marks falsely in connection with spam email, Defendant is likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the email sent by the Kelihos Botnet, including through the Harmful Botnet Domains.

65. As a result of Defendant's wrongful conduct, Defendant is liable to Microsoft for violation of this provision of the Lanham Act.

66. Microsoft is entitled to an injunction against Defendant under the Lanham Act.

67. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

FIFTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

68. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 36 above.

69. The Microsoft Marks are distinctive marks that are associated with Microsoft and exclusively identify Microsoft's business, products, and services.

70. By creating keys and writing entries under a registry path that includes the Microsoft Marks, Defendant is likely to cause dilution by blurring and dilution by tarnishment of the Microsoft Marks. By using the Microsoft Marks, as subdomains or as content available through the Harmful Botnet domains, Defendant is likely to cause dilution by blurring and dilution by tarnishment. By using the Microsoft Marks falsely in connection with spam email, Defendant is likely to cause dilution by blurring and dilution by tarnishment.

71. As a result of Defendant's wrongful conduct, Defendant is liable to Microsoft for violation of this provision of the Lanham Act.

72. Microsoft is entitled to an injunction against Defendant under the Lanham Act.

73. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will

continue unless Defendant's actions are enjoined.

SIXTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

74. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 36 above.

75. Defendant's actions in operating the Kelihos Botnet result in unauthorized access to the computers of Microsoft and its customers and result in unsolicited, bulk electronic mail being sent to, from or through the computers of Microsoft and its customers.

76. Defendant intentionally caused this conduct and this conduct was unauthorized.

77. Defendant's actions have caused injury to Microsoft and its customers and imposed costs on Microsoft and its customers, including time, money and a burden on the computers of Microsoft and its customers, as well as injury to Microsoft's business goodwill and diminished the value of Microsoft's possessory interest in its computers and software.

78. As a result of Defendant's unauthorized and intentional conduct, Microsoft has been damaged in an amount to be proven at trial.

79. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Unjust Enrichment

80. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 36 above.

81. The acts of Defendant complained of herein constitute unjust enrichment of the Defendant at Microsoft's expense in violation of the common law.

82. Defendant accessed, without authorization, computers running Microsoft's software.

83. Defendant used, without authorization or license, the facilities of Microsoft's software to, among other acts, deliver malicious software, support the Kelihos Botnet, deliver unsolicited, bulk email and deliver fake antivirus software.

84. Defendant's actions in operating the Kelihos Botnet result in unauthorized access to the computers of Microsoft and its customers and result in unsolicited, bulk electronic mail being sent to, from or through the computers of Microsoft and its customers.

85. Defendant profited unjustly from the unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers.

86. Defendant had an appreciation and knowledge of the benefit derived from the unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers.

87. Retention by the Defendant of the profits derived from the unauthorized and unlicensed use of Microsoft's software and the computers of Microsoft and its customers would be inequitable.

88. Defendant's unauthorized and unlicensed use of Microsoft's software and use of the computers of Microsoft and its customers have damaged Microsoft in an amount to be proven at trial, and Defendant should disgorge Defendant's ill-gotten profits.

89. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Conversion

90. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 36 above.

91. Defendant has willfully interfered with and converted Microsoft's personal property, without lawful justification, as a result of which Microsoft has been deprived of possession and use of its property.

92. As a result of Defendant's actions, Microsoft has been damaged in an amount to be proven at trial.

93. As a direct result of Defendant's actions, Microsoft has suffered and continues to suffer irreparable harm for which Microsoft has no adequate remedy at law, and which will continue unless Defendant's actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Microsoft prays that the Court:

1. Enter judgment in favor of Microsoft and against Defendant.

2. Declare that Defendant's conduct has been willful and that Defendant has acted with fraud, malice and oppression.

3. Enter a preliminary and permanent injunction enjoining Defendant and Defendant's officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

4. Enter judgment awarding Microsoft actual damages from Defendant adequate to compensate Microsoft for Defendant's activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

5. Enter judgment disgorging Defendant's profits.

6. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial.

7. Enter judgment awarding attorneys' fees and costs, and

8. Order such other relief that the Court deems just and reasonable.

Dated: January 23, 2012

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Christopher M. O'Connell

REBECCA L. MROZ
Va. State Bar No. 77114
CHRISTOPHER M. O'CONNELL
Va. State Bar No. 65790
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
bmroz@orrick.com
coconnell@orrick.com

Of counsel:

GABRIEL M. RAMSEY (admitted *pro hac vice*)
JACOB M. HEATH (admitted *pro hac vice*)
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com

DEMAND FOR JURY TRIAL

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: January 23, 2012

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Christopher M. O'Connell

REBECCA L. MROZ
Va. State Bar No. 77114
CHRISTOPHER M. O'CONNELL
Va. State Bar No. 65790
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Facsimile: (202) 339-8500
bmroz@orrick.com
coconnell@orrick.com

Of counsel:

GABRIEL M. RAMSEY (admitted *pro hac vice*)
JACOB M. HEATH (admitted *pro hac vice*)
Attorneys for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com